FAQ

Maximum number of Managed FortiAPs in FortiOS 5.0.3 FAQ

Background Information

Based on the processing capabilities of each FortiGate model, there is a hard maximum value programmed into FortiOS that restricts the number of FortiAPs that can be managed from a single FortiGate device.

For other maximum values related to wireless (such as maximum number of SSIDs per FortiGate), please refer to the maximum values matrix located in the documentation site http://docs.fortinet.com/fgt/handbook/50/fortigate-max-values-50.pdf (search for "Wireless Controller").

What has changed in FortiOS 5.0.3 that impacts the maximum number of managed FAPs?

FortiOS 5.0.3 introduced the concept of "remote" mode and "normal" mode FAP types. New "Local Bridge Mode" and "Tunnel Mode" SSID types have also been introduced. The addition of the Local bridge mode SSID and remote FAP type has allowed Fortinet to increase the maximum number of FAPs that can be managed by a single FortiGate running FortiOS 5.03 and above.

What is the difference between Tunnel Mode and Local Bridge Mode SSIDs?

Tunnel Mode uses a traditional thin AP architecture, whereby each AP creates both a control and data tunnel to the wireless LAN controller. All wireless traffic traverses that tunnel and is processed by the FortiGate before being passed to the wired LAN.

In contrast, Local Bridge Mode FAPs allow "local" traffic to be bridged directly from the FAP to the wired LAN, without having to traverse the tunnel and be processed by the FortiGate. Only a control tunnel is established between the controller and the FAP in this case, making Local Bridge Mode ideal for many remote locations that do not have a local FortiGate device.

What is the difference between normal and remote mode FAPs?

FAPs configured as 'normal' mode can have both Tunnel *or* Local Bridge Mode SSIDs associated to them. FAPs configured as remote mode can only have Local Bridge Mode SSIDs associated to them.

As Local Bridge Mode does not require wireless LAN data traffic to be processed by the FortiGate, a significantly higher number of remote mode FAPs running Local Bridge Mode SSIDs only can be managed per FortiGate.

Does an FAP change between normal and remote mode automatically?

No. By default, all FAPs are configured as normal mode to allow either Tunnel or Local Bridge Mode SSIDs to be associated with them. There is a CLI configuration command to change FAPs to remote mode if only Local Bridge Mode SSIDs will be associated with it.

To configure an FAP as remote mode, use the `set-wtp remote` command as per the below example:

```
FortiGate # config wireless-controller wtp
FortiGate (wtp) # edit FP223B3X12000426
FortiGate (FP223B3X12000426) # set wtp-mode remote
FortiGate (FP223B3X12000426) # end
FortiGate #
```

This CLI setting has no technical impact on the wireless LAN operation of the FAP, it is simply ensures that only Local Bridge Mode SSIDs can be associated with the FAP.

Once this setting has been configured, you can use the `show wireless-controller wtp` command to confirm that the FAP has been configured as remote mode:

```
FortiGate # show wireless-controller wtp

config wireless-controller wtp
    edit "FP223B3X12000426"
        set name "test-AP-name"
        set wtp-mode remote
        set wtp-profile "test-profile-name"
    next
end

FortiGate #
```

FAPs that have a Tunnel Mode SSID associated to them will throw an error if you attempt to configure them as remote mode from the CLI.

What does the Managed FortiAPs number and status bar in the GUI represent?

The status bar and number in the top right-hand corner of the FortiGate GUI represents the total number of managed FortiAPs on that FortiGate device, in other words, the sum of all normal and remote mode FAPs.

The below screenshot was taken from a FortiGate-100D running FortiOS 5.0.3, which supports a total of 64 FAPs with up to 32 configured in normal mode. As mentioned earlier, FAPs will always be configured as normal mode by default. As a result, this FortiGate will not allow more than 32 FAPs to be managed unless some FAPs are configured as remote mode from the CLI (using the `set wtp-mode` command).

This is important as customers can get confused as to why they cannot manage the number of FAPs that the GUI says they should be able to, if they are unaware that the remote mode setting must be manually configured from the CLI.

What are the Maximum FortiAPs values for each FortiGate model?

Below is a table that shows the maximum number of managed FortiAPs per FortiGate, as well as the maximum number of managed FortiAPs per FortiGate that can be configured in normal mode.

Note: Legacy FortiGate devices that do not support FortiOS 5.0.3 and FortiGate devices that do not support the Wireless Controller feature do not appear on this list.

Wireless Controller Model	Maximum number of managed FortiAPs	Maximum number of managed FortiAPs configured in normal mode
FortiGate/FortiWiFi 20C & 30D	-	-
FortiGate/FortiWiFi 40C, 60C & 60D Series	10	5
FortiGate/FortiWiFi 80C, & 90D Series	32	16
FortiGate 100D, 110C/111C, 200B & 200D Series	64	32
FortiGate 300C, 310B/311B	512	256
FortiGate 620B/621B	512	256
FortiGate 600C, 800C	1,024	512
FortiGate 1000 & 3000 Series	4,096	1,024
FortiGate 5000 Series	Up to 57,344 (4,096/blade)	Up to 14,336 (1,024/blade)
FortiGate VM-eval	1	1
FortiGate VM00	64	32
FortiGate VM01	64	32
FortiGate VM02	512	256
FortiGate VM04	512	256
FortiGate VM08	4096	1024

For example, a FortiGate 100D could manage a maximum of 64 FAPs running in remote mode (if configured with the `set wtp-mode remote` command from the CLI), or a mixture of 32 normal mode and 32 remote mode, but not 64 running in normal mode.

How much bandwidth does the "remote" FAP management tunnel use?

Reducing the management traffic has been a goal of Fortinet to ensure the product uses minimal WAN bandwidth to meet the requirements of distributed installations. The management Capwap Tunnel traffic is a single heartbeat packet sent every 30 seconds. Automatic Radio Resource Provisioning also sends a minimal amount of data every 5 minutes. If necessary, these timers can be adjusted to further decrease the bandwidth utilization.